Title:	Encryption Management	SOP No:	ITS-RADIO-004
Revision:	1.0	Effective Date:	August 1, 2014
Owner:	Manager - Radio Services	Department:	IT Solutions

P25 System Encryption Management

1 Purpose

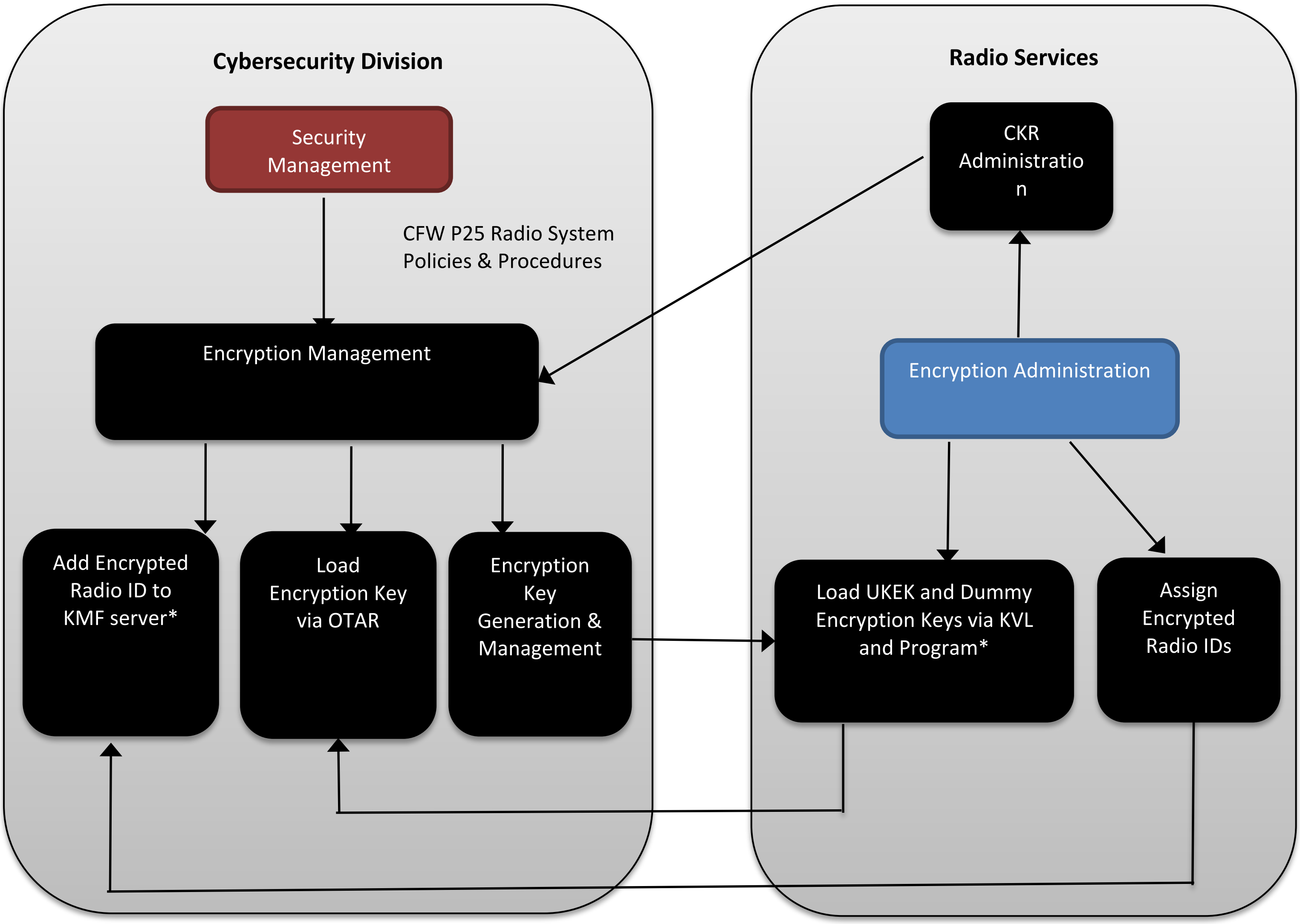
Encryption Management is defined by security policies and procedures governing the management, administration and use of AES encryption on the City of Fort Worth P25 radio system. The objective of P&P 4 is to outline the roles and responsibilities of IT Solutions staff in managing security on the network, but also describe the methodologies for generating, loading, distributing, updating and removing encryption keys as illustrated in Figure 1.

1.1 Security Management

The Cybersecurity Division is responsible for Security Management of the City of Fort Worth P25 radio network including adherence to IT Policy and implementation of security polices and procedures that protect sensitive data and mission critical radio system communications. Consequently, Encryption Management and generating encryption keys are also a Cybersecurity Division duty. The assigned Information Security Analyst will be the Cybersecurity Division point of contact.

1.2 Encyrption Administration

Radio Services is responsible for execution and administration of the security policies and procedures developed by the Cybersecurity Division including administration of Common Key References (CKR's), programming, and removing encryption keys on subscribers. The Communications Manager will be the Radio Services point of contact.



Cybersecurity Division
Security Management
CFW P25 Radio System Policies & Procedures
Encryption Management
Add Encrypted Radio ID to KMF server*
Load Encryption Key via OTAR
Encryption Key Generation & Management
Radio Services
CKR Administratio n
Encryption Administration
Load UKEK and Dummy Encryption Keys via KVL and Program*
Assign Encrypted Radio IDs

Figure 1: Security Management Roles and Responsibilities

**Definitions in Figure 1*
UKEK: Universal Key Encryption Key
KVL: Key Variable Loader
KMF: Key Management Facility Server
OTAR: Over-the-Air Rekeying

2 Scope

All City of Fort Worth AES Encrypted Subscribers on the network must be equipped with OTAR and comply with the policies and procedures in this document.

External agencies with AES encryption, Over-the-Air Rekeying (OTAR) and their own KMF server must maintain software and operating system updates as recommended by Motorola (which are normally updated quarterly) to keep these updates in synchronization with the City of Fort Worth. In addition, adequate protection by industry-standard enterprise grade firewalls with IPS is required.

The Cybersecurity Division will manage Encryption for external agencies in one of the two methods described below.

2.1 *External Agencies with OTAR*

The Interlocal Agreement (ILA) between the City and external agency must reflect inclusion of Encryption Management Services with OTAR.

- Agencies with their own KMF Server and Client will manage their own security policies and encryption keys. External Agencies with OTAR must request their own CKR's from NCTCOG.
- Agencies with OTAR but without a KMF Server and Client will be centrally managed by the Cybersecurity Division.
- Agencies with OTAR using other encryption methodologies aside from AES or in conjunction with it will be handled as an exception.

2.2 *External Agencies without OTAR*

External agencies opting to use AES encryption without OTAR will be addressed on a case by case basis. In this scenario, the ILA will be revised to reflect the specific agreement between the requesting External agency and the City of Fort Worth. CFW will not manage encryption for non-OTAR AES agencies.

3 References

- ITS-RADIO-002 Subscriber Asset Management
- ITS-RADIO-003A New Subscriber Activation
- ITS-RADIO-004 Encryption Management
- ITS-RADIO-006 Lost or Stolen Radio

4 Conditions for Exemption

Exceptions to the policy must be approved by the Senior Manager over Radio Services.

5 Justification

Security polices are critical to protect confidential, sensitive and mission critical communications on the City of Fort Worth P25 radio system.

Encryption key management is necessary to ensure that Public Safety communications remain online, active and fully operational and do not encounter downtime due to incorrect or out of synchronization encryption keys.

6 Encryption Management Rules

This section defines the methodologies for Encryption Management.

6.1 Common Key Reference (CKR)

CKR's are permanent system-wide three-digit key references assigned to talk groups. Each transmission encryption (TEK) key is associated with a CKR. Radio Services manages and maintains a CKR database.

6.2 CKR Administration

North Central Texas Council of Governments (NCTCOG) manages and maintains a regional CKR block assignment list, and has distributed blocks to the City of Fort Worth. The City locally assigns specific CKRs to talkgroups.

6.3 Security Groups

All of the City's subscribers are loaded with CKR's to enable interoperable communications per their specific radio template requirements. Interoperability talkgroups operate in "clear" unencrypted mode of communications.

6.4 Encrypting Subscribers

First, Radio Services will assign radio ID's as defined in Radio 001 and enable them with encryption capabilities. Cybersecurity will then activate these radio ID's with encryption in the KMF server.

Subscribers that require OTAR must first be loaded by an authorized KVL which also contains the Universal Key Encryption Key (UKEK). The UKEK is a single permanent key which cannot be changed. The UKEK and the CKR must be programmed into a Subscriber radio template before Transmission Encryption Keys (TEK) can be loaded.

6.5 Encryption Key Generation

The process for Encryption Key generation and loading is illustrated in Figure 2.

The Cybersecurity Division will use the Pseudo Random Number Generator on the KMF Server to generate TEK's. TEKs will also be randomly assigned to CKRs for additional security. Each CKR is associated with two TEK's, the existing encryption key and the new encryption key which allows the radio to remain functional during a keyset changeover.

6.5 Loading TEK's onto Subscribers

OTAR will be used for all City of Fort Worth encrypted radios and those external agencies with OTAR capabilities that have agreed to the terms of the ILA. The Cybersecurity Division will transmit TEK's from the KMF Server on a scheduled or as needed basis. Subscribers will then be notified to manually Rekey Request so their radios activate on the new TEK.

The manual process illustrated in Figure 2 utilizing a KVL will be used to load TEK's at initial load only. Radio Services will load a "dummy" key with their KVL onto the subscribers as depicted in Figure 1, after which the OTAR process described above will be followed.

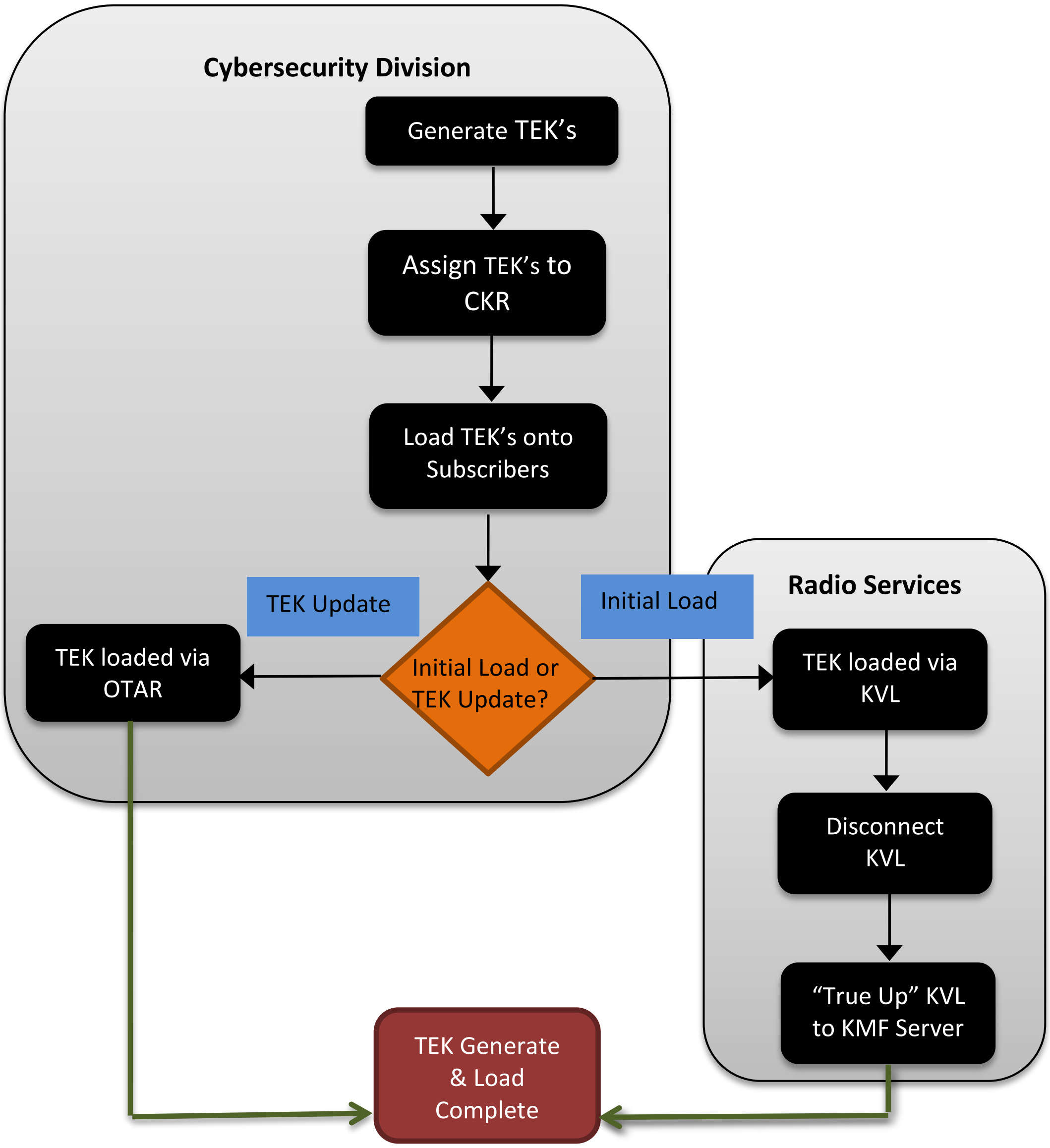


Figure 2: Generation of Encryption Keys and Loading Subscribers

6.7 *Active Period for Encryption Keys*

TEKs will be updated based on specific agency requirements but at least once a year. Radios will need to be rekeyed when TEKs are updated.

6.8 *Schedule for Encryption Key Updates*

When TEKs are updated, the need for rekey will be communicated to external OTAR users by group emails from the Cybersecurity Division. Group emails will be based on a master list of external client POCs with follow-up via phone calls to ensure the need to rekey was received. Users will be informed at Roll Call and advised to rekey their radios by manual rekey request as soon as possible. A thirty day period and three attempts are available for rekey after which the radio will cease to operate in encrypted mode.

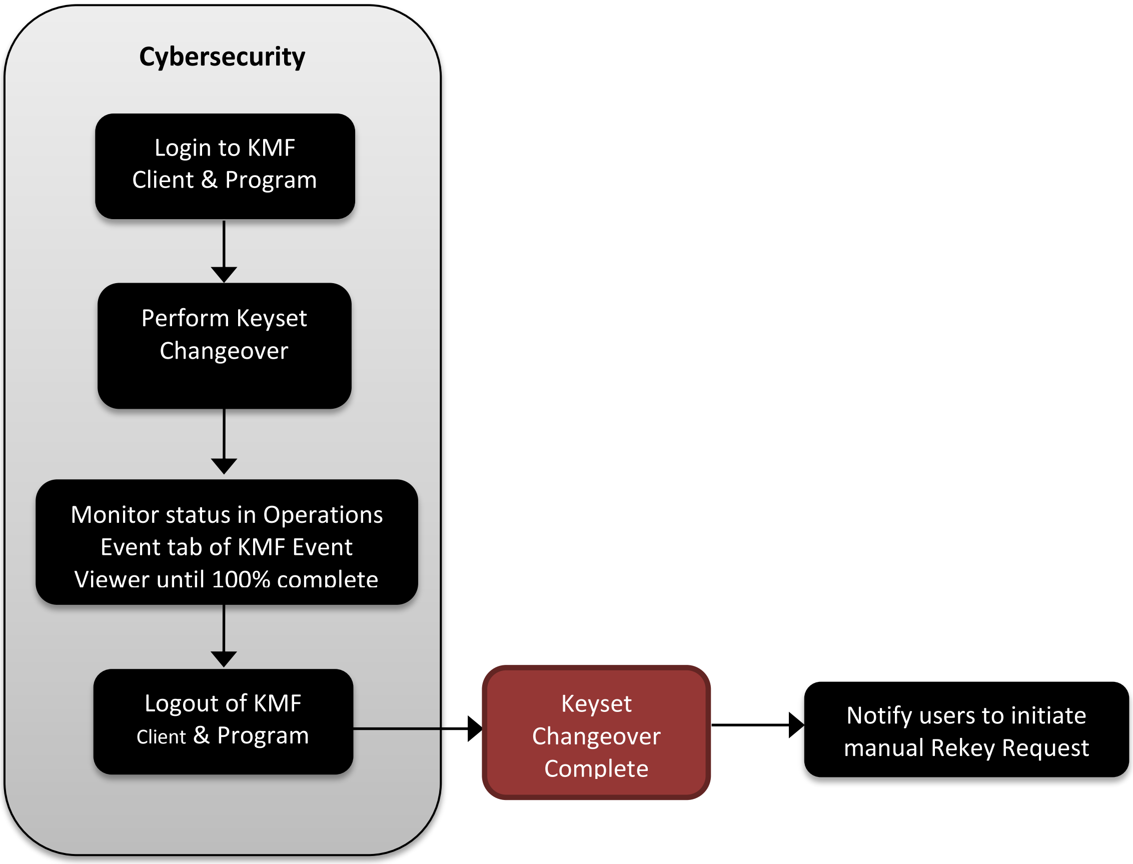

Cybersecurity
Login to KMF Client & Program
Perform Keyset Changeover
Monitor status in Operations Event tab of KMF Event Viewer until 100% complete
Logout of KMF Client & Program
Keyset Changeover Complete
Notify users to initiate manual Rekey Request

Figure 3: OTAR Keyset Changeover Process

6.9 KVL Procedures and Management

External agencies opting to use AES encryption without OTAR will be addressed on a case by case basis. In this scenario, the ILA will be revised to reflect the specific agreement between the requesting External agency and the City of Fort Worth. CFW will not manage encryption for non-OTAR AES agencies.

6.10 Console Encryption Keys

Consoles must be loaded with encryption via Over-the-Ethernet Keying (OTEK). Consoles will be loaded with the UKEK and CKRs at initial load during installation via the KVL. Updates after installation will occur via the OTEK process.

- **<u>OTEK Load of encryption keys on Consoles</u>**

  When TEKs are updated, the need for rekey will be communicated at Shift Change. Dispatchers will be advised to rekey their console position by manual rekey request as soon as possible. A thirty day period and three attempts are available for rekey after which the console will cease to operate in encrypted mode.

- **<u>External Consoles</u>**

  External consoles with City of Fort Worth P25 encrypted talkgroups must also follow the procedure outlined above.

  Similarly, external P25 encrypted talkgroups monitored by CFW consoles would require rekey should their TEKs be updated.

6.11 Disaster Recovery Encryption Management

In an emergency scenario, TEKs will not be updated and encrypted communications will remain online. If necessary, radios can revert to clear mode talkgroups for communication.

To protect against a complete KMF Server failure, database backups are performed quarterly. This backup will consist of running the database backup to the designated folder on the server, then copying the database onto two separate external storage devices. One device will be kept in a safe in the Zipper Bldg. Lab on the second floor and the second will be kept at designated off-site secure storage. Also, every time TEKs are updated, they will be loaded onto a KVL managed by the Cybersecurity Division. Radios could then be manually rekeyed if necessary via the KVL until the KMF Server is restored.

7 Supporting Documentation

Motorola Manual 6871019P56-A *Secure Communications – System Perspective*
Motorola Manual 6871018P43-D *Key Management Facility*
Motorola Manual 6871018P37-C *KVL 4000 Key Variable Loader ASTRO25 User Guide*
Motorola Manual 6871018P34-C *KVL 4000 Quick Start Guide*

Title:	Encryption Management	SOP No:	ITS-RADIO-004
Revision:	1.0	Effective Date:	August 1, 2014
Owner:	Manager - Radio Services	Department:	IT Solutions

Version Control

Version	Date	Description	Author
1.0	8/1/2014	Original version	Abinta Khan